METHOD AND MICROCOMPUTER SYSTEM FOR THE AUTOMATIC, SECURE AND DIRECT TRANSMISSION OF DATA

Publication number: JP2000515332T

Publication date: 2000-11-14

Inventor:

Applicant:

Classification:

- International: ***G06F13/00; G06F15/16; H04L12/56; H04L12/58; H04M3/00; H04M11/00; H04M11/06;*** **G06F13/00; G06F15/16; H04L12/56; H04L12/58; H04M3/00; H04M11/00; H04M11/06;** (IPC1-7): H04M11/00; G06F13/00; H04L12/54; H04L12/58; H04M3/00

- European: H04L12/58; H04M11/06

Application number: JP19970523974T 19961220

Priority number(s): WO1996DE02489 19961220; DE19951049307 19951229

Also published as:

- WO9724825 (A3)
- WO9724825 (A2)
- EP0870386 (A3)
- EP0870386 (A2)
- US6058168 (A1)

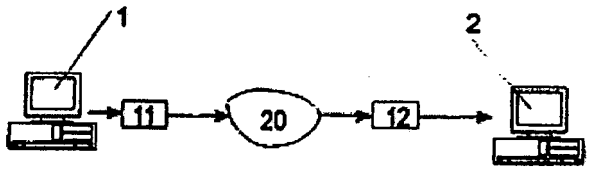
more >>

Report a data error here

Abstract not available for JP2000515332T

Abstract of corresponding document: **WO9724825**

The invention concerns a method for the automatic, secure and direct transmission of data, in particular e-mail. The invention calls for the data to be transmitted from a first terminal (1) to a first microcomputer system (11) which is directly associated with the first terminal (1). The data are processed in the first microcomputer system (11) and immediately or subsequently transmitted directly via a data line (20) to a second microcomputer system (12) which is directly associated with a second terminal (2). The data are processed in the second microcomputer system (12) and immediately or subsequently transmitted to the second terminal (2). The microcomputer systems (11, 12) receive, transmit, store and process data independently of the operational status of the first (1) and second (2) terminals. The invention makes it possible to transmit data directly and automatically, i.e. without the need for a central computer to be connected between the terminals (e.g. PCs) of a data-transmission link. Moreover, with the method and microcomputer system (11, 12) proposed, it is possible to improve data security in numerous ways.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－515332
（P2000－515332A）
(43)公表日　平成12年11月14日(2000.11.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04M	11/00	303	H04M	11/00	303
G06F	13/00	351	G06F	13/00	351G
H04L	12/54		H04M	3/00	B
	12/58		H04L	11/20	101B
H04M	3/00				

審査請求　未請求　予備審査請求　有　（全 55 頁）

(21)出願番号　特願平9－523974
(86)(22)出願日　平成８年12月20日(1996.12.20)
(85)翻訳文提出日　平成10年６月29日(1998.6.29)
(86)国際出願番号　ＰＣＴ／ＤＥ９６／０２４８９
(87)国際公開番号　ＷＯ９７／２４８２５
(87)国際公開日　平成９年７月10日(1997.7.10)
(31)優先権主張番号　１９５４９３０７．９
(32)優先日　平成７年12月29日(1995.12.29)
(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　ティクシ．コム　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング　テレコミュニケイション　システムズ
ドイツ連邦共和国　ベルリン　カルメリーターヴェーク　114
(72)発明者　マーティン　プラバント
ドイツ連邦共和国　ベルリン　カルメリーターヴェーク　114
(74)代理人　弁理士　矢野　敏雄　（外３名）

最終頁に続く

(54)【発明の名称】　自動的で安全かつダイレクトなデータ伝送のための方法およびマイクロコンピュータシステム

(57)【要約】
本発明は、自動的で安全かつダイレクトなデータ伝送、例えば電子メール伝送のための方法に関する。本発明では、第１の端末機器（１）から、該第１の端末機器に直接対応付けされた第１のマイクロコンピュータシステム（１１）にデータが伝送され、該第１のマイクロコンピュータシステム（１１）においてデータが処理され、直ちに又は後の時点で直接データ回線網（２０）を介して第２のマイクロコンピュータシステム（１２）にデータが伝送され、該第２のマイクロコンピュータシステム（１２）は第２の端末機器（２）に直接対応付けされ、該第２のマイクロコンピュータシステム（１２）にてデータが処理され直ちに又は後の時点で第２の端末機器（２）に伝送され、前記マイクロコンピュータシステム（１１，１２）によって、第１の端末機器（１）又は第２の端末機器（２）の作動状態に依存せずにデータの受信、送信、記憶、処理が行れる。

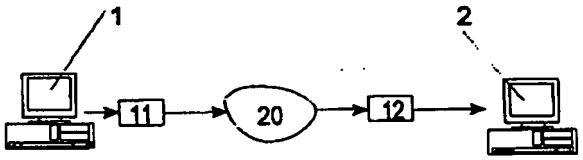


Fig. 2

【特許請求の範囲】

1. 自動的で安全かつダイレクトなデータ伝送、例えば電子メール伝送のための方法において、

a）第１の端末機器（１）から、該第１の端末機器に直接対応付けされた第１のマイクロコンピュータシステム（１１）にデータを伝送し、

b）該第１のマイクロコンピュータシステム（１１）においてデータを処理し、

c）直ちに又は後の時点で直接データ回線網（２０）、例えば電話回線網を介して第２のマイクロコンピュータシステム（１２）にデータを伝送し、該第２のマイクロコンピュータシステム（１２）は第２の端末機器（２）に直接対応付けされたものであり、

d）該第２のマイクロコンピュータシステム（１２）においてデータを処理し、そのデータを直ちに又は後の時点で第２の端末機器（２）に伝送し、

e）前記マイクロコンピュータシステム（１１，１２）によって、第１の端末機器（１）又は第２の端末機器（２）の作動状態に依存せずにデータの受信、送信、記憶、処理を行わせることを特徴とする、自動的で安全かつダイレクトなデータ伝送のための方法。

2. 自動的で直接的かつ安全なデータ伝送、例えば電子メール伝送のための方法において、

a）第１の端末機器（１）から、該第１の端末機器に

直接対応付けされたマイクロコンピュータシステム（１１）にデータを伝送し、

b）該マイクロコンピュータシステム（１１）においてデータを処理し、

c）前記データを直ちに又は後の時点で直接データ回線網（２０）、例えば電話回線網を介して第２の端末機器（２）に伝送し、

d）前記マイクロコンピュータシステム（１１）によって、第１の端末機器（１）の作動状態に依存せずにデータの受信、送信、記憶、処理を行わせることを特徴とする方法。

3. 自動的で直接的かつ安全なデータ伝送、例えば電子メール伝送のための方法において、

a）データを第１の端末機器（１）から、直接データ回線網（２０）、例えば電話回線網を介して、第２の端末機器（２）に直接対応付けされたマイクロコンピュータシステム（１２）に伝送し、

b）該マイクロコンピュータシステム（１２）においてデータを処理し、

c）前記データを直ちに又は後の時点で第２の端末機器（２）に伝送し、

d）前記マイクロコンピュータシステム（１２）によって、第２の端末機器（２）の作動状態に依存せずにデータの受信、送信、記憶、処理を行わせることを特徴とする方法。

4. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つは、データの受信の際に、自動的にメッセージ、例えば受信確認メッセージ又は電子メールの応答メッセージを返信する、請求項１～３いずれか１項記載の方法。

5. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つは、データの圧縮、解凍、暗号化、解読化を行う、請求項１～４いずれか１項記載の方法。

6. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つから送信された及び/又は受信されたデータは優先度に従って処理される、請求項１～５いずれか１項記載の方法。

7. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つによって受信されたデータは、所定の基準、例えば発信者、サイズ、優先情報、対象、コピーかオリジナルかに関してフィルタリング及び/又は分類される、請求項１～６いずれか１項記載の方法。

8. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つに記憶されているデータが、データ回線網（２０）を介して遠隔操作によって処理、例えば転送されるか及び/又は前記マイクロコンピュータシステム（１１，１２）の少なくとも１つの作動状況が遠隔操作によって変更される、請求項１～７いずれか１項記載の方法。

9. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つに記

憶されているデータの遠隔処理の際に、記憶されている情報の所定の部分のみが処理される、請求項１～８いずれか１項記載の方法。

10. 前記マイクロコンピュータシステム（１１，１２）のうちの少なくとも１つのマイクロコンピュータシステムのデータ及び/又は作動状況が、安全性検査（セキュリティチェック）の後でのみ遠隔操作によって処理ないし変更可能である、請求項１～９いずれか１項記載の方法。

11. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つから届いた所定の発信者のデータが拒絶されるか又は受入れられる、請求項１～１０いずれか１項記載の方法。

12. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つによって、所定の発信者の発信者情報の入力が記録され、引き続き自動的に発信者への応答がトリガされ、発信者データの検査の後でのみデータがマイクロコンピュータシステム（１１，１２）に伝送される、請求項１～１１いずれか１項記載の方法。

13. a）前記マイクロコンピュータシステム（１１，１２）の少なくとも１つに届いたデータに、処理及び/又は記憶の前に所定の基準に従った第１の検査を

施し、

b）前記第１の検査の結果がポジティブであった場合にのみマイクロコンピュータシステム（１１，１２）によって処理及び/又は記憶を行わせ、

c）データ回線網（２０）とマイクロコンピュータシステム（１１，１２）の間の接続を、届いたデータの読込みの後で自動的に遮断し、

d）引き続き前記データに、マイクロコンピュータシステム（１１，１２）において所定の基準に従った第２の検査を施し、

e）該第２の検査の結果もポジティブであった場合にのみ、対応付けられている端末機器（１，２）への伝送を行う（データに対する水門式制限方式）、請求項１～１２いずれか１項記載の方法。

14. データ回線網（２０）からマイクロコンピュータシステム（１１，１２

）を介して、対応付けられている端末機器（１，２）へのアクセスを回避させ、それによって端末機器（１，２）への直結的なデータ伝送又はアクセスを不可能にする（端末機器へのアクセスに対する水門式制限方式）、請求項１～１３いずれか１項記載の方法。

15. 前記マイクロコンピュータシステム（１１，１２）の少なくとも１つから送信されたデータに、アドレスデータとして名前と電話番号を与える、請求項１～１４いずれか１項記載の方法。

16. a）端末機器（１，２）との直接接続のための少なくとも１つの第１のインターフェース（５０）と、
b）データ回線網（２０）、例えば電話回線網との接続のための少なくとも１つの第２のインターフェース（５１）と、
c）マイクロコンピュータシステム（１１，１２）の機能の制御のための少なくとも１つのプロセッサシステム（９０）と、
d）伝送データ、オペレーティングシステム、オペレーティングソフトウエアの記憶のための少なくとも１つの記憶素子（８０）と、
e）受信情報、送信情報及び/又は記憶された情報のための指示器及び/又は信号発生器が設けられていることを特徴とする、請求項１～３に記載の方法を実施するためのマイクロコンピュータシステム。

17. 前記少なくとも１つの第２のインターフェース（５１）は、モデム及び/又はＩＳＤＮインターフェース（７０）に接続されている、請求項１６記載のマイクロコンピュータシステム。

18. 前記少なくとも１つの記憶素子（８０）は、ＲＯＭ、フラッシュＲＯＭ、ＲＡＭ、ハードディスク、光学的記憶媒体及び/又はディスクドライブとして構成されている、請求項１６又は１７記載のマイクロコンピュータシステム。

19. 届けられたデータ及び送信されたデータ、例えば電子メールの自律的処理のための手段が設けられている、請求項１６～１８いずれか１項記載のマイクロコンピュータシステム。

20. 所定のメッセージ、例えば受信確認、伝送プロトコル、又は電子メールに対する応答等のメッセージをデータ回線網（２０）を介して自動的に送信する手段が設けられている、請求項１６～１９いずれか１項記載のマイクロコンピュータシステム。

21. 種々の伝送プロトコルとデータフォーマット、例えばファックスデータ、音声データ及び/又は画像データなどに対する変換手段が設けられている、請求項１６～２０いずれか１項記載のマイクロコンピュータシステム。

22. コンピュータネットワークに対するネットワークインターフェースとネットワークソフトウエアが設けられている、請求項１６～２１いずれか１項記載のマイクロコンピュータシステム。

23. 届けられたデータ又は送信されたデータの処理、例えば記憶されたデータの分類、フィルタリング、圧縮、及び/又は暗号化などのための手段が設けられている、請求項１６～２２いずれか１項記載のマイクロコンピュータシステム。

24. 前記マイクロコンピュータシステム(１１，１２)に記憶されたデータの遠隔処理及び/又はマイクロコンピュータシステム（１１，１２）の機能の遠隔操作のための手段が設けられている、請求項１６～２３いずれか１項記載のマイクロコンピュータシステム。

25. 前記マイクロコンピュータシステム（１１，１２）に記憶されているデータに対する不正なアクセス及び/又は前記第１のインターフェース（５０）に接続されている第１の端末機器（１）又は第２の端末機器（２）に対する不正なアクセスを阻止するための手段が設けられている、請求項１６～２４いずれか１項記載のマイクロコンピュータシステム。

26. 所定の発信者から届いたデータの拒絶又は受け入れのための手段が設けられている、請求項１６～２５いずれか１項記載のマイクロコンピュータシステム。

27. 伝送データの発信元を検証するために、所定の発信者からのデータの際に自動的にリターンコールを行う手段が設けられている、請求項１６～２６いず

れか１項記載のマイクロコンピュータシステム。

28. ａ）マイクロコンピュータシステム（１１，１２）における処理及び/又は記憶の前に、届いたデータに所定の基準に従って第１の検査を施す手段と、
ｂ）データ回線網（２０）とマイクロコンピュータシステム（１１，１２）の間の接続を自動的に中断する手段と、
ｃ）マイクロコンピュータシステム（１１，１２）に

おける処理及び/又は記憶されたデータに所定の基準に従って第２の検査を施す手段と、
ｄ）前記第１の検査ないし第２の検査に依存して、データ回線網（２０）からマイクロコンピュータシステム（１１，１２）へのデータ伝送、ないしはマイクロコンピュータシステム（１１，１２）から対応付けられた端末機器（1，2）へのデータ伝送を許可するか又は阻止する手段が設けられている（データに対する水門式制限方式）、請求項１６～２７いずれか１項記載のマイクロコンピュータシステム。

29. データ回線網（２０）からマイクロコンピュータシステム（１１，１２）を通って対応付けされた端末機器（1，2）へのアクセスを阻止する手段が設けられており、それによって直結的なデータ伝送と端末機器（1，2）へのアクセスが不可能にされている（端末機器に対するアクセスの水門式制限方式）、請求項１６～２８いずれか１項記載のマイクロコンピュータシステム。

30. 前記マイクロコンピュータシステム（１１，１２）から送信されるデータに名前と電話番号を添付させる手段が設けられている、請求項１６～２９いずれか１項記載のマイクロコンピュータシステム。

【発明の詳細な説明】

自動的で安全かつダイレクトなデータ伝送のための方法およびマイクロコンピュータシステム

本発明は、自動的で安全かつダイレクトなデータ伝送のための方法およびマイクロコンピュータシステムに関する。

今日、エンドユーザによるコンピュータ（たとえばＰＣ）間で情報を交換することが多くなってきている。この場合、慣用的に純粋なテキスト情報の伝送は”電子メールとして注目されている。そうこうしているうちに、たとえばファックスや音声、画像や映像のデータあるいはたとえばプログラム、データバンクからのデータ、測定データ等その他のコンピュータデータも、コンピュータ間で伝送されるようになってきており、したがって以下では“電子メール”という用語は、いかなる形態であろうとコンピュータ間のデータ交換のことであるものとする。

ここで欠点となるのは、ファックスや電話によるトラヒックとは異なり、電子メールを端末機器のユーザ（たとえばインターネットを経由したＰＣのユーザ）にダイレクトに配達するのは、大きなコストをかけることによってしか実現できないことである。したがって、送信側端末機器と受信側端末機器との間における

ダイレクトな自動データ伝送はきわめて面倒である。それというのも、両方の端末機器または中央コンピュータを一時記憶装置として接続しておかなければならず、スイッチオンされているコンピュータにおいてデータ交換コントロールのための所定のプログラムを実行させなければならないからである。

つまり、中央コンピュータは安全性の理由（たとえばデータの安全性、システム故障に対する安全性）からたいていは別の役割を担うことはできず、日夜作動させていなければならない。このような“常時スタンバイ”システムは今日、たいていは会社内で種々の会社所在地におけるデータ処理ネットワーク間に組み込まれたり（いわゆるルータまたはメールサーバ）、あるいは端末機器をワールドワイドなネットワークたとえばインターネットに接続するために組み込まれる。

現在、電子メールの場合にはたとえば、電子メール伝送のために常時スタンバ

イ状態にある“中継ステーション”を利用できるいわゆる“サービスプロバイダ”に頼らざるを得ない。

公知の方法の場合、電子メールは“送信側郵便局”およびコンピュータ中間ステーションから成るワールドワイドなネットワークを介して、受取人の本来の端末機器とは異なり常時作動中である受信側郵便局まで発送される。また、これらの郵便局は、エンドユーザの直接的な影響範囲内には存在していない。このような郵便局には、端末機器のところにいる受取人が取りに行くまで電子メールがおかれており、その際、受取人は郵便局に規則的に問い合わせなければならず、つまり受取人は自身で措置を講じなければならない。電子メールの本来の伝送は数秒しかかからないのにもかかわらず、現在、緊急郵便をこの経路で送達することはできない。なぜならば送り手にとって、本来の受取人が郵便を取りに行くのか否か、そしていつ取りに行くのかがわからないからである。

しかも、介在接続されている郵便局は常にデータ量が増え続けていることから過負荷になることが多く、その結果、予測外の遅れを伴ってしかデータ伝送を行えないことが多い。このような遅れや受取人のところへの到着の不確かさ、およびインターネットにおけるデータ保護の悪さゆえに、著しく速い電子メールというものに対し相対的に価値がおかれるようになっている。

したがってエンドユーザは現在に至るまで、電話やファックスの回線網などのように完全自動の簡単かつダイレクトで信頼性があり確実な送信側端末と受信側端末間のデータ伝送を利用することができない。

たとえばファックスは今日、電話回線網を介して受取人へダイレクトに最も短期間で送ることができ、この場合、受取人の関与なしに印刷が完了する。しかも送り手に対し、受取人のところにファックスがきちんと届けられたという通報がフィードバックされる。電子メールの公知の伝送方式は、このような利点をもっていない。この理由からもファックスは、その送信が基本的に電子メールの送信よりも遅いにもかかわらず、その意義を保持し続けているのである。

電話による会話の場合もファックスの場合も、データは送信側のエンドユーザから受信側のエンドユーザへダイレクトに伝送され、これは送信者も受信者も第３者の労力を必要とすることなく行われる。

ヨーロッパ特許出願EP 0 671 831 A1から、データ処理機器やデータ再生機器などの端末へ転送すべきデータを受信するための装置が公知である。この場合、端末がオフにされているときにデータが到来すると、この装置は制御信号によって端末機器を動作準備完了状態にさせる。このときデータは少なくとも動作準備完了状態が確立されるまで、一時的に記憶される。この装置の欠点は、端末機器の動作準備完了状態を作り出す点でしか機能しないことである。しかも、現に存在している電子的郵便送達の欠点は、この装置によっても取り除かれない。

論文“Entlastung des zentralen Rechners durch frei programmierbare Nachrichtenuebertragungssteuerungen?”（buero technik Automation+Oraganisation, 11.1972, p. 1348-1356）により、電話回線網を介してエンドユーザのデータステーション（端末、terminal）が接続されている中央コンピュータについて述べられている。この場合、中央コンピュータとデータステーションとの間に制御ユニットが配置されており、このユニットは中央コンピュータの負荷を軽減するために用いられる。その際、制御ユニットは中央コンピュータ（back-end）のための“フロントエンド（front-end）”と呼ばれる。

既述のシステムにおける欠点は、エンドユーザがこの中央コンピュータに完全に依存していることであり、しかもこの中央コンピュータに対しエンドユーザはいかなる影響も及ぼせないことである。したがってたとえば中央コンピュータが故障してしまうと、それに接続されているすべてのエンドユーザは彼らのデータステーションを介してデータを送信することも受信することもできなくなってしまう。しかもエンドユーザにとって、特定のデータをそのデータステーションで読み出すために中央コンピュータに“ログイン”するという手間が増える。それにしても最も深刻な欠点は、特定のデータが“到着”したとき、データステーションまたは中央コンピュータがスイッチオンされていなかったりスタンバイ状態

にない間は、エンドユーザはデータステーションにおいていかなる通報も受け取らないことである。

このような従来技術に基づき本発明の課題は、ダイレクトな自動データ伝送つまりデータ伝送区間の各端

末（たとえばＰＣ）間に中央コンピュータを介在接続させないデータ伝送を可能にし、その際にスイッチオフされている端末機器へもデータを送信できるようにした方法および、この方法を実施するための装置を提供することにある。

この場合、エンドユーザがデータを、中央コンピュータを介在させることなくダイレクトに別のエンドユーザへ送信できるようにすべきであって、受取人の端末機器がスイッチオンされているかされていないかをエンドユーザが知ることなく、あるいは知っている必要なく行えるようにすべきである。

本発明によればこの課題は、請求項１、２または３記載の特徴を備えた方法、および請求項１６の特徴を備えた上記の方法を実施するためのマイクロコンピュータシステムによって解決される。

本発明の方法によれば、端末機器（たとえばエンドユーザのＰＣ）の間に中央コンピュータを介在接続させることなく、データ伝送区間の各端末機器間においてダイレクトで安全かつ自動的なデータ伝送が実現される。ここでいうダイレクトなデータ伝送とは、プロバイダのサービスの手間をとらせることなく、あるエンドユーザから別のエンドユーザへ直接、データが伝送されることを意味する。

この場合、それぞれ１つの端末機器に対し本発明によるマイクロコンピュータシステムがじかに対応づけ

られており、その際、このマイクロコンピュータシステムは、同時に端末機器およびデータ回線網（たとえば電話回線網）と接続されているか、またはデータ回線網とのみ接続されている。後者の場合、端末機器（たとえばラップトップコンピュータ）はマイクロコンピュータシステムから切り離され、したがってマイクロコンピュータシステムはいわば端末機器用の“留守番電話機”として機能することになる。本発明によるマイクロコンピュータシステムは自律的なユニットで

あり、このユニットは端末機器の動作状態とは無関係にデータを受信し、送信し、記憶し、あるいは処理することができる。

ここで端末機器とは一般に、エンドユーザがじかに取り扱うことのできる領域内に存在するコンピュータまたはコンピュータシステムのことである。それらの端末機器には本発明によるマイクロコンピュータシステムのほかに、モニタ、プリンタ、ハードディスク、光学記憶媒体あるいはその他の周辺機器を接続可能である。また、データ伝送ネットワークとしてたとえば公衆電話回線網が使用され、このことによって可用性が高まりかつコストが低下する。

本発明によるマイクロコンピュータシステムは端末機器にじかに配属されて設けられており、たとえばこれは留守番電話機が電話にじかに設けられているようなものである。

その際、マイクロコンピュータシステムから配属されたその端末機器へのデータ伝送、あるいはマイクロコンピュータシステムから他の端末機器へのデータ伝送を、ただちに行うこともできるし、あるいはあとになって行うこともできる。

ただちに行われるデータ伝送の前提条件は、関与しているマイクロコンピュータシステムが作動中であることだけである。とはいうものの、自律的に動作するマイクロコンピュータシステムを使用することにより、受信されたデータおよび／または送信されたデータの処理を、端末機器の動作状態から完全に分離することができる。

マイクロコンピュータシステムは受信されたまたは処理されたデータを、対応づけられた端末機器の動作状態とは無関係に送信する。たとえばエネルギー節約の理由で送り手または受取人の端末機器がスイッチオフ状態にあっても、じかに対応づけられたマイクロコンピュータシステムによってデータを完全に自動的に受信し、処理し、あるいは送信することができる。端末機器はそれに対応づけられて設けられているマイクロコンピュータシステムと常に物理的に接続されていなくてもよく、このことは今日広く普及している移動端末機器にとって殊に重要である。

このようにしてマイクロコンピュータシステムによりたとえば、自動的に別の

を伝送することができ、これはそのために送信端末機器が動作状態にある必要もなく、あるいはそれがマイクロコンピュータシステムと結合されている必要もない。マイクロコンピュータシステムにより受信された電子メールは、対応づけられている端末機器の動作状態とは無関係に処理したり記憶したりすることができる。

マイクロコンピュータシステムにおいて、端末機器から送信されるあるいはその端末機器のためのものであるデータに対し、まえもって規定可能な処理が行われる。マイクロコンピュータシステムにおける記憶がどうしても必要となるのは、対応づけられている受信側端末機器が受け取り準備完了状態になかったり、データ伝送ネットワークを介したデータ伝送速度がマイクロコンピュータシステムと配属された端末機器との間における速度よりも著しくおそいことから、送信すべきデータをただちにデータ伝送ネットワークへ送信できなかったりそうすべきではない場合や、受信データをまずはじめに収集するようにした場合である。

ここで重要であるのは、端末機器に対応づけられているマイクロコンピュータシステムのバッファメモリ容量によって、データ伝送ネットワーク内の“郵便局”による記憶が不要になることである。本発明による方法によれば、送信者から受信者へのダイレクトなデータ伝送が実現され、これはデータ処理またはデータ記憶のためたとえばサービスプロバイダなど別の機関を必要とすることなく実現可能である。送信側や受信側では、データ伝送のためにたとえばメールサーバとのインタラクションなどの特別な措置は不要である。しかしながら、本発明によるマイクロコンピュータシステムは目下利用されているデータ伝送方式と互換性があるので、サービスプロバイダからも電子メールを受信できるし、それに対して電子メールを送信することもできる。

本発明による方法の有利な実施形態によれば、少なくともマイクロコンピュータシステムはデータを受信すると自動的にメッセージを送信する。このように自動的に送信されるメッセージは、たとえば到来データに対する受信確認とするこ

とができる。

さらに有利には、少なくとも１つのマイクロコンピュータシステムによりデータが圧縮され、伸張され、暗号化され、あるいは解読される。データ圧縮により、データネットワークを介して伝送すべきデータ量が著しく低減され、このことにより伝送時間つまりはコストが減少する。さらにデータ圧縮により、マイクロコンピュータシステム内でも僅かな記憶場所しか占有されなくなる。この場合、データがマイクロコンピュータシステムから呼び出されると、たとえば呼び出した場所では伸張を行えない場合、そのデータを自動的に伸張することができる。データ伝送ネットワークを

介して送信されるデータを暗号化することにより、データの安全性が著しく高められ、このことは殊に業務上のトラヒックにおいてきわめて重要である。

この方法の１つの実施形態によれば、マイクロコンピュータシステムにより送信されたおよび／または受信されたデータは、優先順位に従って処理される。この目的で、所定のデータに優先順位情報が設けられており、たとえば”緊急！”や”秘密”などの情報を設けることができる。

本発明による方法のさらに別の有利な実施形態によれば、マイクロコンピュータシステムにより受信されたデータが所定の判定基準に従って分類され、および／または処理される。したがってたとえば特定の差出人から到来したデータを自動的に消去したり、あるいは別のアドレスへ転送したりすることができる。

有利には、マイクロコンピュータシステム内に記憶されたデータが、データ伝送ネットワークを介して遠隔処理される。さらに有利には、マイクロコンピュータシステムの動作が遠隔操作によって制御される。このようにすることで、端末機器が起動していなくても、たとえばマイクロコンピュータシステム内に記憶されているデータを処理できるだけでなく、マイクロコンピュータシステムによる自動処理を制御することができる。このことは、ユーザがかなり長い期間、そのユーザの端末機器およびそれに対応づけられたマイク

ロコンピュータシステムのすぐ近くにいないときに、重要な意味をもつ。この場

合、格別有利であるのは、マイクロコンピュータシステム内に記憶されているデータのうち、まえもって定められた部分だけを処理したり転送したりすることである。このようにすることでたとえば、遠隔制御によりマイクロコンピュータシステム内に記憶されているデータに関する概観を得ることができ、これによって最も重要な電子メール送達物だけを、あるいは短い電子メール送達物だけを、遠隔地に滞在する所属の端末機器のユーザへ伝送することができる。

さらに有利には、特定の識別子（たとえば”秘密”）などの付されたデータをセキュリテイチェック後にはじめて表示させるようにすることもできる。このようにすることで、マイクロコンピュータシステム内に記憶されているデータに対するユーザ・ハイアラーキを構築でき、その結果、特定のユーザはすべてのデータをアクセスできるのに対し、その他のユーザはそれらのデータのうち一部分しかアクセスできないようになる。

本発明による方法のさらに別の有利な実施形態によれば、あらかじめ設定可能な差出人からのデータがマイクロコンピュータシステムに到来したとき、そのデータが拒絶されるか、または許可される。このようにして、たとえば不所望な広告送達物の受信を差し止め

ることができる。

有利には、マイクロコンピュータシステムはあらかじめ設定可能な差出人からのデータの到来を検出し、それを検証するためその差出人へのリターンコールを自動的に発生させる。差出人の検証が成功したあとではじめて、マイクロコンピュータシステムへデータが伝送される。差出人アドレスの検証により、データ伝送におけるセキュリティが改善される。

この方法のさらに別の有利な実施形態によれば、マイクロコンピュータシステムに到来したデータに対しマイクロコンピュータシステムは、あらかじめ設定可能な判定基準による第１のチェックを行う。したがってたとえば特定の差出人からのデータを、マイクロコンピュータシステムが処理する前にただちに拒否することができる。この第１のチェックに従ってデータが許可されると、データはマイクロコンピュータシステム内に格納される。そしてデータ回線網へのマイクロ

コンピュータシステムの接続は、自動的に遮断される。次に、マイクロコンピュータシステム内のデータに対し、あらかじめ設定可能な判定基準による第２のチェック（たとえばウィルスチェック）が行われる。さらにこの第２のチェックにおいて、電子署名の解読または検証も行える。

第２の検査において肯定的な結果が得られたときのみ（たとえばウィルスが存在せず、解読が成功し電子

署名が適正であるときのみ）、マイクロコンピュータシステムに対応づけられた端末機器へデータが伝送される。データに対する水門方式（"floodgate principle"）と呼ばれる２段階のチェックによって、端末機器に対するデータセキュリティが著しく高められる。

さらにこの方法における別の格別有利な実施形態の場合、データ回線網から端末機器へのダイレクトなアクセスは、そのことが対応するマイクロコンピュータシステムにより避けられることで、不可能であるように構成されている。上述の水門方式により、権限のない者がデータ回線網と端末機器とのダイレクトなデータ接続を形成させてしまうのが不可能となる。

本発明による方法のきわめて有利な実施形態によれば、マイクロコンピュータシステムから発信されるデータには名前（たとえばログインネーム）と電話番号がアドレス情報として付される。このような形式のアドレス指定であれば、電子メールの差出人は多数のアドレスを覚えておかなくてもよく、差出人にとって既知である電話番号をアドレスとして使用できる。

ダイレクトな自動データ伝送のための本発明によるマイクロコンピュータシステムは、少なくとも１つの第１のインタフェースを有しており、マイクロコンピュータシステムはこのインタフェースを介して端末機器と接続可能である。さらに少なくとも１つの第２のインタフェースを介してマイクロコンピュータシステ

ムはデータ回線網と接続可能である。データ回線網としてたとえば電話回線網が使用される。また、このマイクロコンピュータシステムは、少なくとも１つのオペレーションコントロール用プロセッサシステムと、オペレーティングソフトウ

ェア、プログラムおよびデータを格納するための少なくとも１つの記憶ユニットを有している。さらにマクロコンピュータシステムは、このシステムにより受信または送信された情報あるいはシステム内に格納されている情報のためのインジケータおよび／または音響的信号発生器を有している。このようにすることで、じかに対応づけられているコンピュータとはまったく無関係にデータ伝送を監視することができる。

種々の周辺機器を備えたコンピュータとは対照的に、このマイクロコンピュータシステムはコンパクトなユニットとして構成することができ、このシステムにおけるプロセッサシステムはフレキシブルにプログラミング可能である。さらにこのマイクロコンピュータシステムは大きなエネルギー負荷（たとえばモニタ）を有していない。

これらの理由から、本発明によるマイクロコンピュータシステムを殊にインテリジェントで自律的なユニットとして、本発明によるデータ伝送方法において使用することができる。その際、本発明の着想および範囲内のこととして挙げられるのは、このようなマイク

ロコンピュータシステムをたとえば、同じ電話回線網と接続されているファックス機器や電話機、留守番電話機、あるいはモデムなどその他の機器内に組み込むことである。

殊に有利な実施形態によれば、前記の第２のインタフェースは内蔵モデムおよび／または内蔵ＩＳＤＮインタフェースと接続されている。このようにして、データ伝送ネットワーク次第で（たとえばＩＳＤＮ電話回線網）、アナログでもディジタルでもデータを交換できる。

有利には、マイクロコンピュータシステムは固有の電流供給部たとえば電源アダプタ、バッテリまたは蓄電池による電流供給部を有しており、したがってマイクロコンピュータシステムは電流供給に関しても自律的である。

さらに有利には、マイクロコンピュータシステムの記憶ユニットは固定値メモリ（ＲＯＭ）、フラッシュＲＯＭ、書き込み／読み出しメモリ（ＲＡＭ）、ハードディスク、光学記憶媒体および／またはディスクドライブとして構成されてい

る。このような形態での記憶ユニットはコンパクトに製造可能であり、しかも大量のデータを格納することができる。

マイクロコンピュータシステムの１つの有利な実施形態によれば、電子メールを自律的に処理するための手段が設けられている。このよな手段によってたとえば、特定の差出人から到来したデータを別の住所へ転送したり、あるいはそれを消去することすら可能であって、このことはマイクロコンピュータシステムに対応づけられている端末機器を必要とすることなく可能である。後者は、電子的なデータ伝送を介した不快なダイレクトメールいわゆる”ジャンクメール（junk-mail）”もその間に処理されることから重要である。

さらに有利にはマイクロコンピュータシステムは、自動的にあらかじめ設定可能なあるいはマイクロコンピュータシステム自身によって生成されるメッセージを送信する手段を有している。つまりたとえば電子メールのための受信確認を自動的に送信することができ、このことはマイクロコンピュータシステムに対応づけられている端末機器あるいはデータ伝送ネットワーク内のシステムを必要とすることなく可能である。

電子メールの場合、多数のデータフォーマットが使われるので、本発明によるマイクロコンピュータシステムがたとえばファックスデータ、音声データおよび／または画像データに対する種々の伝送プロトコルおよび／またはデータフォーマットのための変換手段を備えていると有利である。

本発明によるマイクロコンピュータシステムの格別有利な実施形態によれば、コンピュータネットワークおよびネットワークソフトウェアのためのインタフェースを有している。このようにして、マイクロコンピュータシステムは受信データをネットワーク内のすべてのコンピュータへ転送することができるし、あるいはネットワーク内のあらゆるコンピュータからのデータも受信し、データ回線網を介して受取人へ送達することができる。

有利にはこのマイクロコンピュータシステムは、データの圧縮、伸張、暗号化、解読または変換を行う手段を有している。このような手段によってマイクロコ

ンピュータシステムはそれに対応づけられている端末機器とは無関係に、送信すべきデータや受信データを処理することができる。

さらにまた、マイクロコンピュータシステムの動作および／またはこのシステム内に格納されているデータを、遠隔制御によってコントロールできると有利である。その際にマイクロコンピュータシステムが、このシステム自身および／またはその中に格納されているデータに対する不正なアクセスを回避する手段を備えていると、さらに有利である。このよなセキュリティ措置として挙げられるのは、たとえばパスワードセキュリティおよび／または格納されているデータの自動的な暗号化である。

このマイクロコンピュータシステムのさらに別の有利な実施形態によれば、マイクロコンピュータシステムは、あらかじめ設定可能な差出人から到来したデータを拒否あるいは受理する手段を有している。このこ

とで、そのマイクロコンピュータシステムに対応づけられている端末機器への不所望なデータ伝送を避けることができる。このことは殊に、データ中のコンピュータウィルスからの保護の役割を果たす。

有利には本発明によるマイクロコンピュータシステムは、あらかじめ定めることのできる差出人からのデータであれば、データの出所を検証する目的で自動的なリターンコールをを行わせる手段を有している。この検証により、データセキュリティが著しく高められる。

格別有利には本発明によるマイクロコンピュータシステムは、到来データに対しそれらのデータがマイクロコンピュータシステムに読み込まれる前に、システム内での処理および／または記憶に先立ち所定の判定基準（たとえば差出人アドレス）に従って第１のチェックを行う手段を有している。さらにマイクロコンピュータシステムは、このシステムと対応づけられた端末機器をデータ回線網から完全に分離できるようにする目的で、データ回線網とマイクロコンピュータシステムとの接続を自動的に遮断することのできる手段を有している。さらにまた、このマイクロコンピュータシステムは、このシステム内に格納されているデータに対し所定の判定基準に従って第２のチェック（たとえばウィルスチェック）を

行う手段を有している。マイクロコンピュータシステムはさらに、上述の第１の

チェックまたは第２のチャックに依存してデータ回線網からマイクロコンピュータシステムへの、あるいはマイクロコンピュータシステムから対応づけられた端末機器へのデータ伝送を許可したり阻止したりする手段を有している。このような２段階のチェックによって、データセキュリティが著しく改善される。

別の有利な実施形態の場合、本発明によるマイクロコンピュータシステムは、データ回線網からマイクロコンピュータシステムを通して対応づけられた端末機器へのアクセスを阻止する手段を有している。この手段は、マイクロコンピュータシステム内に格納されているプログラムまたは特別にプログラミングされたプロセッサとすることができる。このようにして、ダイレクトなデータ伝送や端末機器のアクセスが不可能となる（端末機器へのアクセスに対する水門閉鎖方式）。

同様に有利には、本発明によるマイクロコンピュータシステムは、発信データに名前（たとえばログインネーム）と電話番号をアドレス情報として設けるための手段を有しており、このことで発信データのアドレス指定をきわめて簡単に行えるようになる。

次に、図面を参照しながら複数の実施例に基づき本発明について詳細に説明する。

図面

図１は、インターネットを介した電子メールの従来

の通常の伝送方法を概略的に示した図である。

図２は、本発明による電子メールの伝送方法を概略的に示した図である。

図３は、本発明によるマイクロコンピュータシステムの概略図である。

図４は、マイクロコンピュータシステムに送信されたデータのセキュリティチェックのためのフローチャートを示した図である。

実施例

図１にはこれまでの通常の電子メールの伝送方法が示されている。この“電子

メール”の概念のもとでは、この場合例えばバイナリフォーマット、テキストフォーマット、画像フォーマット、音声フォーマット、ビデオフォーマットなどのデータが挙げられる。

この電子メールは、第１の端末機器１と第２の端末機器２の間で伝送される。図をわかりやすくするために、ここで選択されている例では第１の端末機器１が送信器として示され第２の端末機器２は受信器として示されている。以下ではデータ伝送区間の端部におけるそれぞれの端末機器を送信器ないし受信器と称するものとする。基本的にはこの送信器１と受信器２は入れ替わってもよいし、あるいはこれらの両端末機器１，２がデータを同時に送受信することも可能である。

送信器１と受信器２は、この実施例では通常の例えばプリンタ、ディスプレイなどの周辺装置が接続され

ているパーソナルコンピュータである。

送信器１と受信器２は、それぞれ伝送装置１ａ，２ａ（例えばモデム）を介して電話回線網２１，２２と接続されている。

これまでの方式による電子メールでは、送信器１から受信器２への直接の伝送は不可能であったので、送信器１からは電話回線網２１を介して“送信側郵便局３１”として機能する、つまりデータを転送したり場合によっては一次的に保管したりするコンピュータへの接続が形成されていた。それに対しては例えば前記送信側郵便局として機能するいわゆるサービスプロバイダの電話番号が呼び出されなければならなかった。しかしながらそのような機能の充足のためには、送信側郵便局３１が常時スタンバイ状態におかれていなければならず、これは著しい管理の手間とそれに伴うコストの増加を意味する。送信側郵便局への接続が確立された後では電子メールが送信側郵便局３１へ伝送される。

送信側郵便局３１からは電子メールがワールドワイドネットワーク４０に伝送される。このネットワークは、不特定多数のネットで結ばれた多数のコンピュータからなっている。この場合電子メールが経由する正確な経路は明確にはわからない。特に電子メールがワールドワイドネットワーク４０内で種々のコンピュータに一時的に記憶されることは通常行われている。

このことは電子メールの伝送時間を増加させるだけではなく、データセキュリティの低下も招く。なぜなら一時的な記憶の際には常に不特定の第３者による電子メールへの不正なアクセスの危険性がつきまとうからである。

ワールドワイドネットワーク４０からは電子メールが受信側郵便局３２として機能するコンピュータに転送される。この受信側郵便局３２も前記送信側郵便局３１と同じように常時スタンバイされていなければならず、これもコスト負担増加の一因となる。

ここにおいてこの電子メールは、受信器２より伝送装置２ａを介してこの受信側郵便局３２への明確な問合わせがなされるまでは、該受信側郵便局３２に保管される。このアクセスは図１中に湾曲した矢印で示されている。

受信器２は、電子メール文章の到着に関する情報の郵便局（サービスプロバイダ）からの通達は何も受けない。このことは今日でのインターネットにおける決定的な欠点となっている。メールの受け取りに対しては、受信器２は固有のステップを踏まなければならず、しかもこれは自身へのメールが本当に存在しているか否かがわからないまま行われなければならない。このような方式では電子メールの交換に対して送信器１から受信器２への中断のない安全でダイレクトなデータ伝送は存在し得ない。

しかしながら現在のデータ受信の通常の形態はインターネットである。このような方式での唯一の例外は、受信者がインターネットへの高価な常時回線を稼動させているか又は受信器がデータの到着の際に偶然にその郵便局（プロバイダ）への接続を形成した場合である。この２つのケースに限っては、受信者はデータを郵便局（プロバイダ）への到着後に直接受け取ることができる。

総じて言えることは、これまでの電子メール交換のもとでは、多くの段階が踏まれなければならず、このことは煩雑な管理と不所望な遅延やコストの負担増加、セキュリティの問題等を引き起こす。特に電子メールアイテムの場合には、今日の電話機では問題なく可能である自動応答装置（オートアンサ）による自動受信も容易ではない。

ファックス送信の場合データは、一次記憶ステーションでの呼び出しの必要な

く直接受信器に伝送される。この場合の唯一の前提条件は、アンサー装置又はファックス装置が常時スタンバイ状態で電話回線網に接続されていることである。

図２には本発明による方法が示されている。ここでも図１と同じように送信器１から受信器２までの電子メールの伝送が示されている。この場合送信器１と受信器２の入れ替えは基本的に可能である。この送信器１と受信器２は、この実施例ではデータ伝送区間の端

部におけるパーソナルコンピュータ（端末機器）であり、これは通常の周辺機器、例えばプリンタ、ディスプレイと接続されている。しかしながら本発明の考察では、ＬＡＮ内のコンピュータも送信器１又は受信器２として使用可能である。

本発明による方法を用いた電子メールの自動的なダイレクト伝送は、本発明によるマイクロコンピュータシステム１１，１２と電話回線網２０を介して行われる。

この場合送信器１には第１のマイクロコンピュータシステム１１が直接対応付けされ、受信器２には第２のマイクロコンピュータシステム１２が直接対応付けされている。すなわち送信器１も受信器２も端末ユーザーとして直接それぞれの対応付けされたマイクロコンピュータシステム１１，１２にアクセスされる。

送信器１に対応付けされた第１のマイクロコンピュータシステム１１は、送信器１と常時接続されている必要はなく、送信器１とデータ交換すべき場合にのみ接続される。この送信は例えば送信器１の送信優先度に依存して自主的に及び/又は電話料を優先する有利な活用のために時間制御されて行われる。

受信器２に対応付けられた第２のマイクロコンピュータシステム１２も受信器２と常時接続されている必要はなく、これは例えば受信器２が接続されていない又は受信準備されていない場合でも電子メールを受け

取ることができる。受信器２がスタンバイ状態か又は接続された場合には、マイクロコンピュータシステム１２は受信器２に電子メール到着に基づくデータ送信の希望を通報してくる。それに応じて受信器２はデータをすぐに受け取るか又は後から受け取る。

すなわちマイクロコンピュータシステム１１，１２は、自律的に常時電話回線網２０と接続された機器であり、これらは送信器１ないし受信器２の空間的近傍に配設される。いずれにせよ送信器１のユーザー又は受信器２のユーザーは、それぞれの対応付けされたマイクロコンピュータシステム１１，１２に対し第３者の仲介なしに直接アクセスできる。

マイクロコンピュータシステム１１，１２はいくつかのプロセッサシステム９０と、電流給電部１００と記憶素子８０を有している（図３）。そのためこれらは対応付けされている送信器１ないし受信器２の作動状態には完全に依存しない。従って例えば受信器２は第２のマイクロコンピュータシステム１２から完全に切り離されていてもよく、この場合は届いた電子メールが第２のマイクロコンピュータ１２によって記憶され処理される。それ故にデータ回線網における一次的な保管（例えば図１中の受信側郵便局３２）は不必要である。本発明による機能は、マイクロコンピュータシステム１１，１２のプロセッサシステム９０と関連させて説明する。

以下ではデータ伝送のシーケンスを説明する。送信器１の端末ユーザーが受信器２の端末ユーザーに伝言を送信したい場合には、送信すべきデータに受信器２の名前とその電話番号を添えて固定のフォーマットで例えば以下のように準備する。

Name+CiybtrtCide-Citycode-Phone Number

Hans.Meier+49-30-4019001

送信器１に対応付けされているマイクロコンピュータシステム１１は、予め設定可能な時点で、アドレスに添えられている受信器２の電話番号をダイヤリングし、それに伴って受信器２のマイクロコンピュータシステム１２とのデータ接続が形成される。その際実質的にはモデムテクノロジから公知の、データ伝送レート、通信プロトコル、データ圧縮設定に対する規約が適用される。

この接続形成の実施の後では、マイクロコンピュータシステム１１，１２の間でパラメータの交換が行われる。その際には受信側マイクロコンピュータシステム１２がアドレスデータを所定のリストと比較する。このリストには、拒否すべ

きリスト（ネガティブリスト）と受入れるべきリスト（ポジティブリスト）が記憶されている。

前記ネガティブリストは、不所望な電子メールの伝送を避けるために用いられる。前記ポジティブリストは、所定のユーザーサークル内だけの端末機器１，２

へのデータ伝送の許容に用いられる。この両手段はコンピュータウイルス（これは例えばテキストファイルも感染し得る）に対する保護の増強に用いられる。届いたデータは、ポジティブリストに掲載されている発信者からのものだけ受け入れられる。それにより他の不要な全てのデータは、既に接続形成開始時点で排除され接続から外される。

パラメータブロックには送信器１がその端末機器に入力されている名前と電話番号の情報が含まれている。タイムゾーンと送信時間に関する情報は、次のことに用いられる。すなわちこのデータ伝送が所定の時間でのみ許容されるようにするために用いられる。パラメータブロック自体に関する情報は、データ伝送におけるデータ保護のために用いられる。マイクロコンピュータシステム１１，１２間のパラメータ交換の際に伝送されるデータブロックは、以下の構造を有している。

データ容量 (Byte)	データ内容
2	パラメータブロックの長さ
１５	国番号－都市番号－電話番号
１５	名前
1	タイムゾーン
4	送信時間
2	パラメータブロック毎のチェッ

クサム

パラメータ交換の成功した後では、送信側マイクロコンピュータシステム１１が受信側マイクロコンピュータシステム１２を所定の命令を介して制御する。こ

の場合命令セットは、“データ受信”と“接続中断”の命令を含んでいる。選択的な実施形態では、特に遠隔操作のもとでは、この命令セットにさらなる命令が含まれていてもよい。

受信側マイクロコンピュータ１２がデータ伝送に対する準備を整えた場合には、これは相応の命令を送信側マイクロコンピュータ１１に送信する。これらのデータは、（プロバイダの）ホストコンピュータによる中間記憶なしで問題なくダイレクトに端末ユーザーに伝送される。その際比較的大きなＬＡＮ内の端末ユーザーはアドレスに添えられている名前（例えばログインネーム）によって同定可能である。

電子メールのヘッダには、受信側マイクロコンピュータ１２がそれに基づいてデータの後続処理を制御する情報が含まれている。特に電子メールのヘッダにはメールの容量とそのタイプ（例えば圧縮又は暗号化されている場合等）に関する情報が含まれている。ヘッダは優先度に関する情報も有している。そのため届いたデータはマイクロコンピュータシステムにより優先度に従って分類される。さらにヘッダは、タイムゾーンと時間表示に関する情報も含んでおり、それによってメールの受信が一義的に定められる。またヘッダは自身に関する情報も含んでおり、それにより伝送データの完全性に関する検査が実施可能である。伝送される電子メールのヘッダは、以下の構造を有している。

データ容量 (Byte)	データ項目
2	ヘッダの容量
4	電子メールの容量
1	電子メールのタイプ
1	優先度識別子
1	タイムゾーン
4	時間表示
2	ヘッダチェックサム

マイクロプロセッサ１２が電子メールを受け取った場合には、自動的な肯定応

答を電子メールの送信器１に送信し、それによって直ちに、電子メールがエラーなしで受信器２に、すなわち受信器２に対応付けられたマイクロコンピュータシステム１２のもとに届いた旨が通達される。

データ伝送が終了した後では、マイクロコンピュータシステム１１，１２が電話回線網から分離される。

受信側マイクロコンピュータシステム１２のローカルメモリが目下のところ尽きた場合には、送信側マイクロコンピュータシステム１１へ次のような命令が伝達される。すなわち後の時点でのデータ伝送を要求す

る命令が伝達される（オートマッチックオプションリピート）。基本的にデータ受信の可能性がない場合には、オートマチックオプションリピートが無意味であることが伝送される。データ伝送の際になんらかのエラーが発生した場合には、このエラーにより、新たなデータ送信を促す命令が伝達される。

さらなるセキュリティの増強に対してマイクロコンピュータシステム１１，１２は、ウイルスに対する着信データの検査プログラムを有している。

その他にもこのマイクロコンピュータシステム１１，１２は、所定の発信者からのデータの着信を記録しデータ発信者への自動応答を行うプログラムを有している。この自動応答によって偶発的な接続エラーの存在が皆無となることが保証される。

またこの自動応答によっては、データの発信者が例えばポジティブないしネガティブリストとの比較によって確証される。この確証がなされるまでは受信側端末機器２のユーザーによるデータの受入れもまだであるが、データ接続が形成された場合にはデータが伝送可能になる。

また、受信側端末機器２に対応付けられたマイクロコンピュータシステム１２は、確証の後でデータ発信者自体からのデータを検索することも可能である。ポジティブリスト上の発信者のアドレスが誤って用いられているデータ発信者もリターンコール過程のもとで

は達成することができない。発信者の同定は、発信者のコンピュータが接続され

る電話番号を介して行われる。

リターンコール機能によっては受信側端末機器２が全ての受信データに関する完全なコントロールを有するようになる。このことはデータセキュリティを著しく高める。

図２に示されている実施例では、２つの端末機器の間、詳細には送信器１と受信器２の間での本発明による電子メールの伝送が表されている。この場合これらの両端末機器にはそれぞれ１つのマイクロコンピュータシステム１１，１２が直接対応付けられている。本発明の考察の一部として、複数のマイクロコンピュータシステム１１，１２が送信側端末機器１ないし受信側端末機器２に対応付けられてもよい。さらに本発明の考察のさらなる展開として唯１つの端末機器１，２に本発明による１つのマイクロコンピュータシステム１１，１２が対応付けられるようなデータ伝送も可能である。それによりこの本発明による方法は、今日の通常のデータ伝送方式との互換性を有するようになる。重要なことは、データ交換に寄与する端末機器１，２のもとで、少なくとも作動状態とデータ交換ないしデータ処理状態の間の分離が可能であることである。

マイクロコンピュータシステム１１，１２は常時データ伝送のために使用可能であるので、それらは他の

システム（例えばヒータや盗難防止装置など）の遠隔制御にも適用することができる（これらのシステムもマイクロコンピュータシステム１１，１２と接続される）。それにより所定の信号、例えばクリア電子メールがヒータ等のスイッチオン/オフのためにマイクロコンピュータシステム１１，１２に送信可能である。

またマイクロコンピュータシステム１１，１２はデータやメッセージも送信可能なので、それに接続されたシステムから他のシステムへの通達も直接伝送可能である。例えばこのマイクロコンピュータシステム１１，１２に接続されているヒーターシステムにおいてエラーが発生した場合には、通報が保守サービス会社に自動的に送信される。盗難防止装置がマイクロコンピュータシステム１１，１２に接続されている場合には、アラームのトリガーの際に警察に自動的に通報が送られる。

また外部からはこのマイクロコンピュータシステム１１，１２を介して所望のシステムの状態が問い合わせ可能である。それにより例えば保守会社は、マイクロコンピュータシステム１１，１２を介してエラー通知が届いているヒータシステムの状態レポートを要求することができる。

図３には本発明によるマイクロコンピュータシステム１１，１２の構造が概略的に示されている。以下では簡単化の理由から実質的にマイクロコンピュータシステム１２に絞って説明を行う。このマイクロコンピュータシステム１２はここでは図示されていない受信器２に対応付けされている。送信器１に対応付けされているマイクロコンピュータシステム１１も基本的に同じ構成であり、そのためマイクロコンピュータシステム１１，１２は、データの送信にも受信にも適用することができる。伝送に対してＩＳＤＮ方式が適用されている場合には両方の過程を同時に行うことができる。

マイクロコンピュータシステム１２は、ここでは図示されていない受信器と電話回線網２０との接続形成のためにインターフェース５０，５１，５２を有している。

このマイクロコンピュータシステム１２の回路は基本的に４つの電子構成群６０，７０，８０，９０からなっており、これらは相互にインターフェース５０，５１，５２と接続されている。符号１００で概略的に示されているのはマイクロコンピュータシステム１２の自律的な電流給電部１００である。この電流給電部は一方では通常の電流網への接続部からなり、他方ではバッテリシステムへの接続部からなる。このバッテリシステムは輸送の際又は回路網遮断の際の電流給電を保証する。機器内部には大きな電流負荷は設けられていないので、典型的にはマイクロコンピュータシステム１２は０．１～１Ｗの線路容量を有している。

このマイクロコンピュータシステム１２は第１のインターフェース５０を介して受信器２と接続され、第２のインターフェース５１を介して電話回線網２０と接続される。また第３のインターフェースを介して外付けモデムが接続可能である。

ＲＳ２３２タイプの第１のインターフェース５０はコンピュータインターフェース６０に接続されている。このインターフェースは受信器２とマイクロコンピュータシステム１２の間のデータ伝送を制御し監視する。他の選択的な実施形態ではこの第１のインターフェース５０がＳＣＳＩインターフェース、赤外線インターフェース、無線インターフェース、又はパラレルインターフェースで構成される。データ交換の制御の際には例えばＸモデムプロトコルが適用される。

記憶素子８０は、プロセッサシステム９０と接続されている。図示の実施例では、この記憶素子内に４ＭＢの記憶容量を有するＲＡＭチップが設けられている。また必要に応じてのメモリ増設のための差込スペースも設けられている。さらに選択的実施例においては、ハードディスクやフロッピーディスクドライブが付加的記憶素子８０として用いられてもよい。本発明の考察では、場合によっては外部記憶媒体がマイクロコンピュータシステム１２に接続されてもよい。このことは特に大量のデータ伝送の際に利点となる。

プロセッサシステム９０は、マイクロコンピュータシステム１２の機能を制御する。この場合はオペレーティングシステムがマイクロコンピュータシステム１２内に記憶されている。このオペレーティングシステムはマルチタスク環境で、そのため複数のデータ伝送が同時に可能である。プロセッサシステム９０は、高級言語でプログラミング可能である。選択的実施例として、データ伝送ネットワーク及び/又は対応付けされた端末機器に対し複数のパラレルコネクタが設けられていてもよい。

マイクロコンピュータシステム１２のプログラミングは、対応付けされた端末機器２を介して行うことができる。しかしながらここでは図示されていない遠隔操作、例えば電話又はリモートコンピュータなどを介してプログラミングを実施することも可能である。その場合には、保安上の理由から遠隔操作のもとで必要に応じてマイクロコンピュータシステム１２の一部だけがプログラミング可能となる。

マイクロコンピュータシステム１２の機能性は、記憶素子８０に記憶されているプログラムによって非常に幅広い要求に適合化される。例えば現存のデータ伝

送方式又はサービスプロバイダーからの提供方式が適用可能である。それによりこのマイクロコンピュータシステム１２は送信器１からのデータを受信し得る。これは対応するマイクロコンピュータシステム１１は有していない。

マイクロコンピュータシステムには、データ圧縮ないしデータ解凍、データ符号化ないしデータ復号化ないしデータ変換のためのプログラムが記憶されており、これらのプログラムはプロセッサシステム９０によってそのつどの要求に応じて使用される。これらのプログラムによってデータは、マイクロコンピュータシステム１２において作動状態に全く依存せずに、あるいは対応付けられる受信器２の有無にかかわらず処理され得る。

特に重要なのは、マイクロコンピュータシステム１２のデータの不正な読み取り又は操作を回避する手段である。それに対しては特にパスワードシステムが用いられる。

基本的にマイクロコンピュータシステム１２はいわゆる“ファイヤウォールコンピュータ”として使用可能である。これは対応付けされる端末機器２に対して大きな防御を提供する。電話回線２０から対応する端末機器２ないしはこれに接続された他のコンピュータへの直接のアクセスはマイクロコンピュータシステム１２によって不可能となる。

それによりこのマイクロコンピュータシステム１２は、到来したデータをまずマイクロコンピュータシステム１２だけに届ける水門のような役目を果たす。

図４には、このような“水門式制限方式”によるマイクロコンピュータシステム１２の動作がフローチャートで示されている。データ回線網２０からマイクロコンピュータシステム１２へデータが伝送されている場合には、第１の検査ステップにおいてデータの発信者アドレスが確認される。但しこの第１の検査はコードワードやその他の基準に関するものである。この発信者がネガティブリストに載っていない場合には、このデータがマイクロコンピュータシステム１２に記憶される。しかしながら発信者アドレスがネガティブリストに載っている場合には、そのデータが排除される

。この場合データの入力の試みがマイクロコンピュータ１２によって記録される。

第１の検査のパスとマイクロコンピュータシステムへのデータの記憶が終わった後では、外部電話回線網２０とマイクロコンピュータシステム１２との間の接続が解除される（モデムの遮断）。

この電話回線網２０とマイクロコンピュータシステム１２との間の接続が遮断された後で初めてこのデータがマイクロコンピュータシステム１２によってウイルス感染に関する第２の検査を試みられる。このウイルスチェックを無事に通過した後で初めて端末機器２への接続が形成され、データがこの端末機器２に伝送される。前記データの第２の検査がネガティブな場合には、このデータが消去され、当該受信器がマイクロコンピュータシステム１２からデータの拒絶に関するメッセージと発信者に関するデータを受け取る。

このようにしてまず最初に電話回線網２０からマイクロコンピュータシステム１２への接続が行われ、その後でマイクロコンピュータシステム１２から対応する端末機器２への接続が行われるように、常に“水門の扉”のみが開かれるだけである。この水門式制限機能によって外部データ回線網２０（例えば電話回線網）から直接端末機器２への接続が無造作に行われることはない。それにより不正な第３者（例えばハッカー）による端末機器２への直接のアクセスは完全に排除される。

マイクロコンピュータシステム１２の制御プログラムは、ＲＯＭ又はＥＰＲＯＭに記憶される。それによりマイクロコンピュータシステム１２を操るためのプログラム変更は不可能となる。

電子メールの量は増加し続けるので、マイクロコンピュータシステム１２内には届いたメールをフィルタリングし分類するプログラムが記憶される。マイクロコンピュータシステム１２内のこのプログラムはどのデータを通過させどのデータは通過させないかを決定する。この手段によって安全性が著しく高められる。

分類基準としては、例えば到来する電子メールの大きさ、発信者、日付、対象などが利用される。それにより例えば特に大きな電子メールはマイクロコンピュ

ータシステム１２によって排除され得る。

例えば即座に通過させるべき電子メールの発信者リストが記憶されている。承認されない発信者の場合には、マイクロコンピュータシステム１２によって自動的に応答が発信者に返信され、電子メールの送達が達成されなかった旨のメッセージが届けられ、場合によっては代替アドレスが与えられる。

その他にも付加的なシークレットコードを電子メールの所定の発信者に割り当てることも可能である。それによりこのシークレットコードを有するメールだけはマイクロコンピュータシステム１２によってどんな場合でも完全に受け入れられるようになる。

マイクロコンピュータシステム１２は、データに送信優先度又は受信優先度の識別子を備えさせる手段も有している。それにより、所定のデータを電話回線網２０に伝送すべき場合にはその送信優先度を介して決定が下される。これによってデータは即座に送信されるか又は予め設定可能な時点で送信されるようになる。例えばマイクロコンピュータシステム１２はデータ伝送に対して自動的に低料金の時間帯を求めることもできる。これにより所定のデータは特に低料金の課金レートで送信される。所定の発信者へのデータは、所期の時間帯にまとめることも可能であり、これによって特に低料金の課金レートで一度にまとめて送信することが可能となる。このことは多岐の時間帯に亘る電子メールの最も効率のよい処理につながる。

受信優先度の識別子を用いることによって、届いた電子メールの処理が効率よく行われる。それにより例えば受信器２のもとで特に重要性を知らせるためには電子メールの所定の発信者に高い優先度が与えられる。

さらにマイクロコンピュータシステム１２は、データ伝送コストを監視する手段を有している。これによりそのつどの電子メールによって落とされたコストが記憶される。そのため実際に落とされたデータ伝送コストに関する目下の情報が

得られる。コストは所定のカテゴリ（例えば所定の送信アドレス又は送信時間）に従って分散させることも可能である。問合わせに対して又は所定の時点においてコストデータを電子メールシステムの管理人に伝達することも可能である。

プロセッサシステム９０は、ＩＳＤＮコントローラ７０に接続されている。このコントローラ７０は電話回線網２０へのデータの伝送を監視し制御する。このＩＳＤＮコントローラ７０の制御はＣＡＰＩを介して行われる。マイクロコンピュータシステム１２の選択的な実施例では、モデムか又はこのモデムとＩＳＤＮ接続端子の組み合わせが用いられる。電話回線網２０へのデータの伝送は第２のインターフェース５１を介して行われる。この第２のインターフェース５１はＩＳＤＮコントローラ７０に接続されている。プロセッサ９０は、その他にインターフェースコントローラ６１を介して第３のインターフェース５２に接続されている。この第３のインターフェースを介して外付けモデムが接続可能である。

本発明は前述してきた実施例にのみ限定されるものではない。それどころか本発明では多くの変化例が可能であり、これらは本発明による方法やマイクロコンピュータシステムによって基本的に他の形式による実施形態にも適用可能である。

【図1】

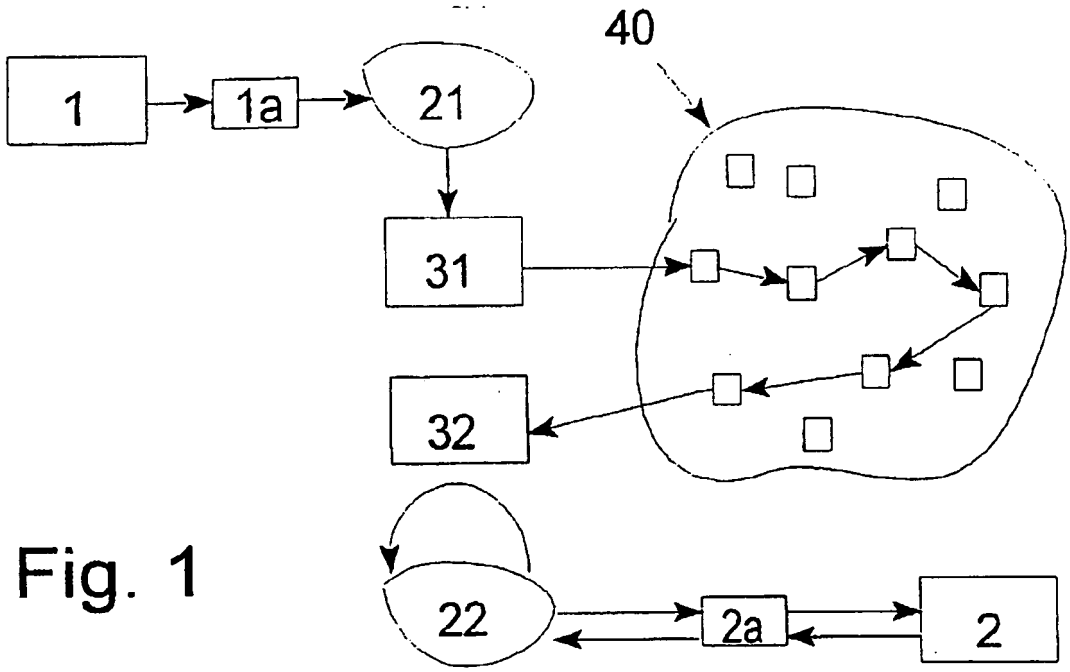


Fig. 1

【図2】

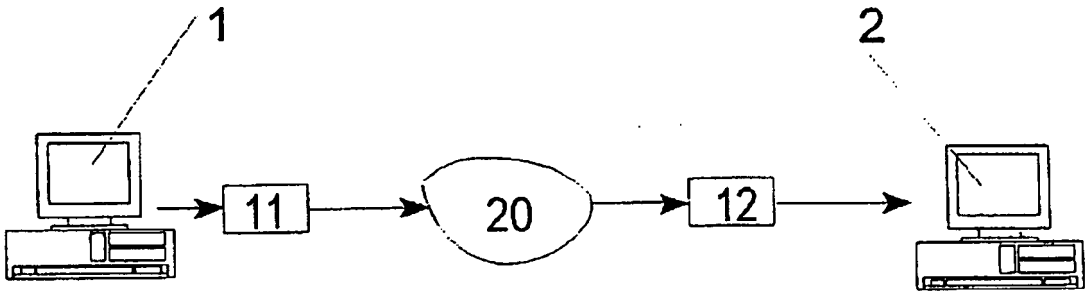


Fig. 2

【図３】

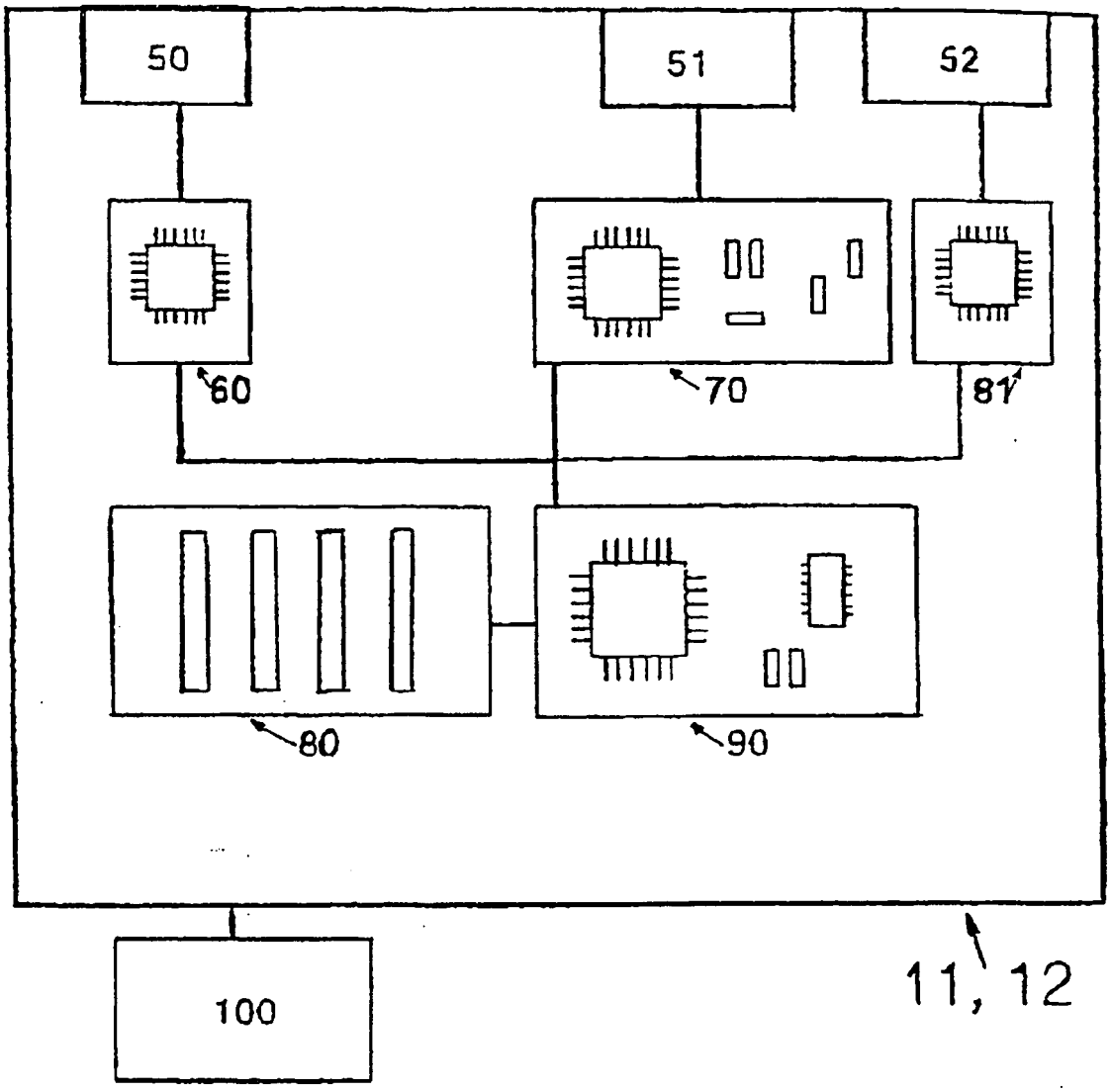


Fig. 3

【図４】

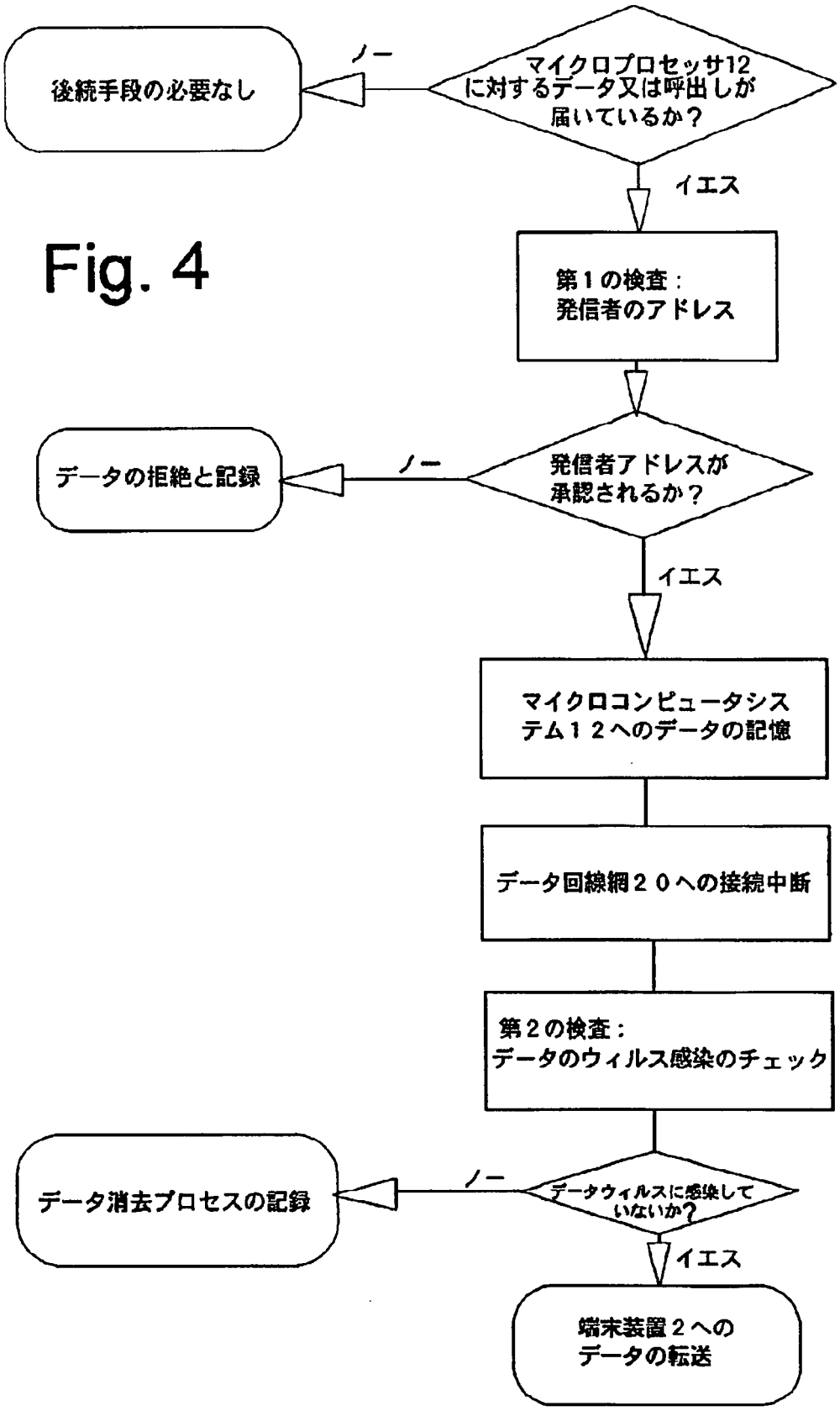

後続手段の必要なし
ノー
マイクロプロセッサ12
に対するデータ又は呼出しが
届いているか？
イエス
第１の検査：
発信者のアドレス
データの拒絶と記録
ノー
発信者アドレスが
承認されるか？
イエス
マイクロコンピュータシス
テム１２へのデータの記憶
データ回線網２０への接続中断
第２の検査：
データのウィルス感染のチェック
データ消去プロセスの記録
ノー
データウィルスに感染して
いないか？
イエス
端末装置２へ
データの転送

Fig. 4

【手続補正書】特許法第１８４条の８第１項
【提出日】平成１０年３月１３日（１９９８．３．１３）
【補正内容】
既述のシステムにおける欠点は、エンドユーザがこの中央コンピュータに完全に依存していることであり、しかもこの中央コンピュータに対しエンドユーザはいかなる影響も及ぼせないことである。したがってたとえば中央コンピュータが故障してしまうと、それに接続されているすべてのエンドユーザは彼らのデータステーションを介してデータを送信することも受信することもできなくなってしまう。しかもエンドユーザにとって、特定のデータをそのデータステーションで読み出すために中央コンピュータに”ログイン”するという手間が増える。それにしても最も深刻な欠点は、特定のデータが”到着”したとき、データステーションまたは中央コンピュータがスイッチオンされていなかったりスタンバイ状態にない間は、エンドユーザはデータステーションにおいていかなる通報も受け取らないことである。

刊行物”Electronic Mailbox”Electronics &; Wireless World Bd. 91, No. 1594, 8.1985, Surrey, p.3338から、２つの端末機器間のダイレクトな電子データ伝送が公知である。この場合、各端末機器に対応づけられたマイクロコンピュータシステムが用いられ、その際、マイクロコンピュータシステムは端末機器の動作状態とは無関係に到来データをバッファリングすることができる。この場合、２つの端末機器間のダイレクトなデータ伝送以外に、データ伝送や端末機器のセキュリティを高めることのできる措置や機構については述べられていない。

国際公開WO-A-93/20647には、データ回線網と端末機器との間に接続されているマイクロコンピュータシステムが開示されている。これによれば、このマイクロコンピュータシステムは殊に、到来データおよび発信データをバッファリングし、異なるデータフォーマット間の変換を行うように構成されている。この文献からも、セキュリティ対策について読み取ることはできない。

アメリカ合衆国特許US-A-5 379 349には、端末に到来するデータに関して、それが完全に伝送された否かについて検査する通信システムが開示されている。こ

の場合、ログファイルが形成され、これは到来データに対する一種の受信確認証としての役割を果たす。それ以外にはこの文献には、データセキュリティを高める手段は開示されていない。

このような従来技術に基づき本発明の課題は、２つの端末機器間におけるダイレクトな情報伝送のための方法および装置において、一方の端末機器が不所望なあるいは有害なデータを受信しないようことのほか保護されるようにして、データ伝送および端末機器のセキュリティが高められるように構成することにある。

本発明によればこの課題は、請求項１記載の特徴を備えた方法、および請求項１６記載の特徴を備えた上

記の方法を実施するためのマイクロコンピュータシステムによって解決される。

本発明の方法によれば、データ伝送区間における２つの端末機器（たとえばエンドユーザのＰＣ）の間におけるダイレクトなデータ伝送が実現される。ここでいうダイレクトなデータ伝送とは、プロバイダのサービスの手間をとらせることなく、あるエンドユーザから別のエンドユーザへ直接、データが伝送されることを意味する。

この場合、受信機器すなわち第２の端末機器に対し本発明によるマイクロコンピュータシステムがじかに対応づけられており、その際、このマイクロコンピュータシステムは、同時に端末機器およびデータ回線網（たとえば電話回線網）と接続されているか、またはデータ回線網とのみ接続されている。後者の場合、端末機器（たとえばラップトップコンピュータ）はマイクロコンピュータシステムから切り離され、したがってマイクロコンピュータシステムはいわば端末機器用の”留守番電話機”として機能することになる。本発明によるマイクロコンピュータシステムは自律的なユニットであり、このユニットは端末機器の動作状態とは無関係にデータを受信し、送信し、記憶し、あるいは処理することができる。

ここで端末機器とは一般に、エンドユーザがじかに取り扱うことのできる領域内に存在するコンピュータ

またはコンピュータシステムのことである。第２の端末機器には本発明によるマ

イクロコンピュータシステムのほかに、モニタ、プリンタ、ハードディスク、光学記憶媒体あるいはその他の周辺機器を接続可能である。また、データ伝送ネットワークとしてたとえば公衆電話回線網が使用され、このことによって可用性が高まりかつコストが低下する。

本発明によるマイクロコンピュータシステムは端末機器にじかに配属されて設けられており、たとえばこれは留守番電話機が電話にじかに設けられているようなものである。

自律的に動作するマイクロコンピュータシステムを使用することにより、受信データの処理を端末機器の動作状態と完全に分離できる。

マイクロコンピュータシステムは、対応づけられた端末機器の動作状態とは無関係にデータを受信しまたは処理する。たとえばエネルギー節約の理由で受取人の端末機器がスイッチオフ状態にあっても、じかに対応づけられたマイクロコンピュータシステムによってデータを完全に自動的に受信または処理することができる。端末機器はそれに対応づけられて設けられているマイクロコンピュータシステムと常に物理的に接続されていなくてもよく、このことは今日広く普及している移動端末機器にとって殊に重要である。

自律的に動作するマイクロコンピュータシステムを

使用することにより、受信データの処理を第２の端末機器の動作状態と完全に分離できる。

マイクロコンピュータシステムは、対応づけられた端末機器の動作状態とは無関係にデータを受信しまたは処理する。たとえばエネルギー節約の理由で受取人の端末機器がスイッチオフ状態にあっても、じかに対応づけられたマイクロコンピュータシステムによってデータを完全に自動的に受信、処理または送信することができる。端末機器はそれに対応づけられて設けられているマイクロコンピュータシステムと常に物理的に接続されていなくてもよく、このことは今日広く普及している移動端末機器にとって殊に重要である。

このようにしてマイクロコンピュータシステムによりたとえば、自動的に別のコンピュータへメッセージを伝送することができ、これはそのために送信端末機

器が動作状態にある必要もなく、あるいはそれがマイクロコンピュータシステムと結合されている必要もない。マイクロコンピュータシステムにより受信された電子メールは、対応づけられている端末機器の動作状態とは無関係に処理したり記憶したりすることができる。

マイクロコンピュータシステムにおいて、端末機器のためのものであるデータに対し、まえもって規定可能な処理が行われる。マイクロコンピュータシステムにおける記憶がどうしても必要となるのは、対応づけられている受信側端末機器が受け取り準備完了状態になかったり、データ伝送ネットワークを介したデータ伝送速度がマイクロコンピュータシステムと配属された端末機器との間における速度よりも著しくおそいことから、送信すべきデータをただちにデータ伝送ネットワークへ送信できなかったりそうすべきではない場合や、受信データをまずはじめに収集するようにした場合である。

ここで重要であるのは、端末機器に対応づけられているマイクロコンピュータシステムのバッファメモリ容量によって、データ伝送ネットワーク内の”郵便局”による記憶が不要になることである。本発明による方法によれば、送信者から受信者へのダイレクトなデータ伝送が実現され、これはデータ処理またはデータ記憶のためたとえばサービスプロバイダなど別の機関を必要とすることなく実現可能である。送信側や受信側では、データ伝送のためにたとえばメールサーバとのインタラクションなどの特別な措置は不要である。しかしながら、本発明によるマイクロコンピュータシステムは目下利用されているデータ伝送方式と互換性があるので、サービスプロバイダからも電子メールを受信できる。

ダイレクトな自動データ伝送のための本発明によるマイクロコンピュータシステムは、少なくとも１つの第１のインタフェースを有しており、マイクロコンピュータシステムはこのインタフェースを介して端末機器と接続可能である。さらに少なくとも１つの第２のインタフェースを介してマイクロコンピュータシステムはデータ回線網と接続可能である。データ回線網としてたとえば電話回線網が使用される。また、このマイクロコンピュータシステムは、少なくとも１つのオ

ペレーションコントロール用プロセッサシステムと、オペレーティングソフトウェア、プログラムおよびデータを格納するための少なくとも１つの記憶ユニットを有している。さらにマクロコンピュータシステムは、このシステムにより受信または送信された情報あるいはシステム内に格納されている情報のためのインジケータおよび／または音響的信号発生器を有している。このようにすることで、じかに対応づけられているコンピュータとはまったく無関係にデータ伝送を監視することができる。

種々の周辺機器を備えたコンピュータとは対照的に、このマイクロコンピュータシステムはコンパクトなユニットとして構成することができ、このシステムにおけるプロセッサシステムはフレキシブルにプログラミング可能である。さらにこのマイクロコンピュータシステムは大きなエネルギー負荷（たとえばモニタ）

を有していない。

これらの理由から、本発明によるマイクロコンピュータシステムを殊にインテリジェントで自律的なユニットとして、本発明によるデータ伝送方法において使用することができる。その際、本発明の着想および範囲内のこととして挙げられるのは、このようなマイクロコンピュータシステムをたとえば、同じ電話回線網と接続されているファックス機器や電話機、留守番電話機、あるいはモデムなどその他の機器内に組み込むことである。

有利にはマイクロコンピュータシステムは、自動的にあらかじめ設定可能なあるいはマイクロコンピュータシステム自身によって生成されるメッセージを送信する手段を有している。つまりたとえば電子メールのための受信確認を自動的に送信することができ、このことはマイクロコンピュータシステムに対応づけられている端末機器あるいはデータ伝送ネットワーク内のシステムを必要とすることなく可能である。

電子メールの場合、多数のデータフォーマットが使われるので、本発明によるマイクロコンピュータシステムがたとえばファックスデータ、音声データおよび／または画像データに対する種々の伝送プロトコルおよび／またはデータフォー

マットのための変換手段を備えていると有利である。

同様に有利には、本発明によるマイクロコンピュータシステムは、発信データに名前（たとえばログインネーム）と電話番号をアドレス情報として設けるための手段を有しており、このことで発信データのアドレス指定をきわめて簡単に行えるようになる。

次に、図面を参照しながら複数の実施例に基づき本発明について詳細に説明する。

【手続補正書】特許法第１８４条の８第１項
【提出日】平成１０年４月１日（１９９８．４．１）
【補正内容】

セキュリティを高めるため、本発明による方法はいくつかの特別なステップを有している。この場合、受信側の端末機器すなわち第２の端末機器に到来したデータは、マイクロコンピュータシステムにより所定の判定基準に従ってチェックされる。

この第１のチェックが成功裏に終わってはじめて、到来データがマイクロコンピュータシステムにより処理され、あるいは記憶される。この第１のチェックは第１のセキュリティステップを成しており、これによって、権限のない者がデータを受信側の端末機器に送ったり、あるいはそれどころか端末機器にアクセスしてしまうことが防止されることになる。この場合、マイクロコンピュータシステムは、それにじかに対応づけられている第２の端末機器の動作状態とは無関係にはたらく。

データセキュリティをさらに改善するため、マイクロコンピュータシステムにデータが読み込まれた後、マイクロコンピュータシステムがデータを受信したデータコネクションが遮断される。データコネクションが終了してはじめて、端末機器へデータを伝送できる状態となる。このようにすることで、端末機器とデータ回線網とがじかに接続することがなくなる。したがってたとえば、確立されているデータコネクションを介して端末機器へのアクセスを取得しようとするハッカーなどにとって、端末機器を操作しようと企むこと

が不可能となる。

本発明による方法によれば、マイクロコンピュータシステムにより読み込まれたデータは、あらかじめ定めることのできる動作モードおよび／または第２の所定の判定基準による遮断後にはじめて処理される。データに対する水門方式（sluice principle）と呼ばれるこのような２段階のチェックないし処理によって、端末機器のためのデータセキュリティが著しく高められる。

本発明による方法の有利な実施形態によれば、あらかじめ定めることのできる差出人から、マイクロコンピュータシステムに到来したデータは、拒絶されるからまたは許可される。この場合、たとえば電話番号から差出人を識別することができる。このようにして、たとえば望ましくない宣伝用メールの受信を抑圧できる。

また、第２のチェックにおいて、電子署名の解読または検証を行うこともできる。第２のチェックにおいて肯定的な結果が得られたときのみ（たとえば解読が成功し電子署名が適正であるときのみ）、マイクロコンピュータシステムに対応づけられた端末機器へデータが伝送される。

この方法のさらに別の有利な実施形態によれば、マイクロコンピュータシステムに読み込まれたデータがコンピュータウィルスに関してチェックされる。これにより、マイクロコンピュータシステムに対応づけられた端末機器へ状況次第では危険なデータが到達してしまうのが防止される。

さらに有利には、マイクロコンピュータシステムによりデータが圧縮され、伸張され、暗号化され、あるいは解読される。データ圧縮により、データネットワークを介して伝送すべきデータ量が著しく低減され、このことにより伝送時間つまりはコストが減少する。さらにデータ圧縮により、マイクロコンピュータシステム内でも僅かな記憶場所しか占有されなくなる。この場合、データがマイクロコンピュータシステムから呼び出されると、たとえば呼び出した場所では伸張を行えない場合、そのデータを自動的に伸張することができる。データ伝送ネットワークを介して送信されるデータを暗号化することにより、データの安全性が著しく高められ、このことは殊に業務上のトラヒックにおいてきわめて重要である

。

この方法の１つの実施形態によれば、マイクロコンピュータシステムにより受信されたデータは、優先順位に従って処理される。この目的で、所定のデータに優先順位情報が設けられており、たとえば”緊急！”や”秘密”などの情報を設けることができる。

本発明による方法のさらに別の有利な実施形態によれば、マイクロコンピュータシステムにより受信されたデータが所定の判定基準に従って分類され、および／または処理される。したがってたとえば特定の差出人から到来したデータを自動的に消去したり、あるいは別のアドレスへ転送したりすることができる。

さらにこの方法における別の格別有利な実施形態の場合、データ回線網から端末機器へのダイレクトなアクセスは、そのことが対応するマイクロコンピュータシステムにより不可能にされることで、行うことができないように構成されている。上述の水門方式により、権限のない者がデータ回線網と端末機器とのダイレクトなデータ接続を形成させてしまうのが不可能となる。

本発明による方法のきわめて有利な実施形態によれば、第１の端末機器から発信されるデータには名前（たとえばログインネーム）と電話番号がアドレス情報として付される。このような形式のアドレス指定であれば、電子メールの差出人は多数のアドレスを覚えておかなくてもよく、差出人にとって既知である電話番号をアドレスとして使用できる。

本発明による方法の１つの有利な実施形態によれば、マイクロコンピュータシステムはデータを受信すると自動的にメッセージを送信する。このように自動的に送信されるメッセージは、たとえば到来データに対する受信確認とすることができる。

有利には、マイクロコンピュータシステム内に記憶されたデータが、データ伝送ネットワークを介して遠隔処理される。さらに有利には、マイクロコンピュータシステムの動作が遠隔操作によって制御される。このようにすることで、端末機器が起動していなくても

、たとえばマイクロコンピュータシステム内に記憶されているデータを処理できるだけでなく、マイクロコンピュータシステムによる自動処理を制御することができる。このことは、ユーザがかなり長い期間、そのユーザの端末機器およびそれに対応づけられたマイクロコンピュータシステムのすぐ近くにいないときに、重要な意味をもつ。この場合、格別有利であるのは、マイクロコンピュータシステム内に記憶されているデータのうち、まえもって定められた部分だけを処理したり転送したりすることである。このようにすることでたとえば、遠隔制御によりマイクロコンピュータシステム内に記憶されているデータに関する概観を得ることができ、これによって最も重要な電子メール送達物だけを、あるいは短い電子メール送達物だけを、遠隔地に滞在する所属の端末機器のユーザへ伝送することができる。

さらに有利には、特定の識別子（たとえば”秘密”）などの付されたデータをセキュリティチェック後にはじめて表示させるようにすることもできる。このようにすることで、マイクロコンピュータシステム内に記憶されているデータに対するユーザ・ハイアラーキを構築でき、その結果、特定のユーザはすべてのデータをアクセスできるのに対し、その他のユーザはそれらのデータのうち一部分しかアクセスできないようになる。

有利には、マイクロコンピュータシステムはあらかじめ設定可能な差出人からのデータの到来を検出し、それを検証するためその差出人へのリターンコールを自動的に発生させる。差出人の検証が成功したあとではじめて、マイクロコンピュータシステムへデータが伝送される。差出人アドレスの検証により、データ伝送におけるセキュリティが改善される。

さらに本発明による方法の実施形態において有利には、データがマイクロコンピュータシステムに読み込まれたとき、マイクロコンピュータシステムのインジケータおよび／または音響的信号発生器により指示が行われる。このことにより、端末機器がスイッチオフ状態であってもユーザは、その端末機器に対応づけられているマイクロコンピュータシステムにデータが送達されたか否かを識別することができる。

さらに本発明による装置は、あらかじめ定めることのできる判定基準に従って到来データに対し第１の検査を行うことのできるチェック手段と、データ回線網を遮断することのできる手段を有している。これらの手段によってデータセキュリティが著しく改善される。

さらに本発明による装置は、データ回線網とマイクロコンピュータシステムとの間の接続を自動的に遮断することのできる遮断手段を有している。さらに本発明によるマイクロコンピュータシステムは、マイクロコンピュータシステムに読み込まれたデータを、あらかじめ設定可能な処理モードおよび／またはあらかじめ設定可能な第２の判定基準に従って処理することのできる処理手段も有している。このことにより、データ回線網からマイクロコンピュータシステムを通して、じかに対応づけられている端末機器へダイレクトにアクセスが行われる可能性がなくなる。

マイクロコンピュータシステムの１つの有利な実施形態によれば、マイクロコンピュータシステムは、あらかじめ設定可能な差出人から到来したデータを拒絶または受諾するチェック手段を有している。このようにすることで、マイクロコンピュータシステムに対応づけられた端末機器への望ましくないデータ伝送を避けることができる。このことは殊に、データ中のコンピュータウィルスからの保護の役割を果たす。

格別有利には、本発明によるマイクロコンピュータシステムは、マイクロコンピュータシステム内に記憶されているデータをコンピュータウィルスに関してチェックすることのできる処理手段を有している。このような付加的なチェックにより、データセキュリティがいっそう高められる。

有利にはこのマイクロコンピュータシステムは、データを圧縮、伸張、暗号化、解読または変換するための処理手段を有している。この手段によりマイクロコンピュータシステムは、それに対応づけられている端末機器とは無関係に、発信すべきデータおよび受信すべきデータを処理することができる。

さらに有利には、マイクロコンピュータシステムの動作モードおよび／またはこのシステム内に格納されているデータを、遠隔操作によってコントロール可能

である。

請求の範囲

1　送信器（1）としての第1の端末機器（1）と、受信器（2）としての第2の端末機器（2）の間でデータ回線網（２０）を介して自動的かつダイレクトなデータ伝送、例えば電子メールの伝送を行うための方法であって、

データ伝送が、前記第2の端末機器に直接対応付けされたマイクロコンピュータシステム（１２）を介して行われ、該マイクロコンピュータシステム（１２）は、対応付けされた第2の端末機器（2）の作動状態に依存せずにデータを受信、送信、記憶、又は処理する形式のものにおいて、

a）前記マイクロコンピュータシステム（１２）に届いたデータに、処理及び/又は記憶の前に、所定の第1の基準に従った第1の検査を施し、

b）前記第1の検査のポジティブな結果の後でのみ前記データをマイクロコンピュータシステム（１２）に読み込み、

c）届いたデータを読み込んだ後でデータ回線網（２０）とマイクロコンピュータシステム（１２）との間の接続を自動的に遮断し、

d）前記マイクロコンピュータシステム（１２）に読み込んだデータをまず所定の処理モード及び/又は所定の第2の基準に従って処理し、

e）引き続き前記マイクロコンピュータシステム（１２）に対応付けされた第2の端末機器（2）に前記データを伝送することを特徴とする自動的かつダイレクトなデータ伝送のための方法。

2.　前記マイクロコンピュータシステム（１２）のもとに届いたデータ、所定の発信者のデータを検査する際に、発信者アドレスに基づいて拒絶又は受入れを行う、請求項1記載の方法。

3.　読み込んだデータに、第2の所定の基準に従った第2の検査を施し、該第2の検査のポジティブな結果の後でのみ、第2の端末機器（2）にデータを転送する、請求項1又は2記載の方法。

4.　前記第2の検査は、読み込んだデータのコンピュータウイルスに関する検

査である、請求項３記載の方法。

5. 前記マイクロコンピュータシステム（１２）に読み込まれたデータを処理によって圧縮、解凍、符号化、復号化する、請求項１～４いずれか１項記載の方法。

6. 前記マイクロコンピュータシステム（１２）によって読み込まれたデータを優先度に従って処理する、請求項１～５いずれか１項記載の方法。

7. 前記マイクロコンピュータシステム（１２）によって読み込まれたデータを処理の枠内で所定の第２の基準、例えば発信者、サイズ、優先度情報、対象、

コピーかオリジナルか等に従ってフィルタリング及び/又は分類する、請求項１～６いずれか１項記載の方法。

8. データ回線網（２０）からマイクロコンピュータシステム（１２）を通って直接対応付けされている第２の端末機器（２）へのアクセスを不可能にし、それによって直結的なデータ伝送又は第２の端末機器への直結的なアクセスをできなくする、請求項１～７いずれか１項記載の方法。

9. 第２の端末機器（２）に直接対応付けられているマイクロコンピュータシステム（１２）に対し、第１の端末機器（１）から送信されたデータに、アドレスデータとして名前と電話番号を添付する、請求項１～８いずれか１項記載の方法。

10. 前記マイクロコンピュータシステム（１２）により、データ受信の際に自動的にメッセージ、例えば受信確認又は電子メールの応答メッセージなどを返信する、請求項１～９いずれか１項記載の方法。

11. 前記マイクロコンピュータシステム（１２）に記憶されたデータを、データ回線網（２０）を介して遠隔操作により処理、例えば転送し、及び/又は前記マイクロコンピュータシステム（１２）の処理モードを遠隔操作によって変更する、請求項１～１０いずれか１項記載の方法。

12. 前記マイクロコンピュータシステム（１２）

に記憶されているデータの遠隔処理の際に、記憶されている情報の所定の一部の

みを処理する、請求項１～１１いずれか1項記載の方法。

13. 前記マイクロコンピュータシステム（１２）の読み込まれているデータ及び/又は処理モードを、遠隔操作によるセキュリティチェックの後でのみ処理可能ないし変更可能にする、請求項１～１２いずれか１項記載の方法。

14. 前記マイクロコンピュータシステム（１２）によって所定の発信者からの発信者情報の入力を記録し、引き続き発信者へのリターンコールを自動的に実施し、発信者データの検査の後でのみデータをマイクロコンピュータシステム（１２）に伝送する、請求項１～１３いずれか１項記載の方法。

15. 前記マイクロコンピュータシステム（１２）に読み込まれたデータを、該マイクロコンピュータシステム（１２）の指示器及び/又は音響的信号発生器によって指示する、請求項１～１４いずれか１項記載の方法。

16. 前記端末機器（1，2）との直接接続のための少なくとも１つの第１のインターフェース（５０）と、

データ回線網（２０）との接続のための少なくとも１つの第２のインターフェース（５１）と、

マイクロコンピュータシステム（１１，１２）の機

能の制御のための少なくとも１つのプロセッサシステム（９０）と、

伝送データ、オペレーティングシステム、オペレーティングソフトウエアの記憶のための少なくとも１つの記憶素子（８０）と、

受信情報、送信情報及び/又は記憶された情報のための指示器及び/又は信号発生器とを有している、請求項１に記載の方法を実施するためのマイクロコンピュータシステムにおいて、

a）マイクロコンピュータシステム（１１，１２）における処理及び/又は記憶の前に、届いたデータに所定の第１の基準に従って第１の検査を施す検査手段と、

b）データ回線網（２０）とマイクロコンピュータシステム（１１，１２）の間の接続を自動的に遮断する遮断手段と、

c）マイクロコンピュータシステム（１１，１２）に読み込まれたデータのみに

、所定の動作モード及び/又は所定の第２の基準に従って処理を施す処理手段とが設けられており、データ回線網（２０）からマイクロコンピュータシステム（１１，１２）を通って直接対応付けされている端末機器（１，２）への直結的アクセスが不可能にされていることを特徴とする、マイクロコンピュータシステム。

17. 前記検査手段は、届いたデータを発信者アドレスに基づいて拒絶又は受入れる、請求項１６記載のマイクロコンピュータシステム。

18. 前記処理手段は、読み込まれたデータをコンピュータウイルスに関して検査する、請求項１６記載のマイクロコンピュータシステム。

19. 前記処理手段は、読み込んだデータの処理として、例えばデータの分類、フィルタリング、圧縮及び/又は暗号化を行う、請求項１６～１８いずれか１項記載のマイクロコンピュータシステム。

20. 前記処理手段は、マイクロコンピュータシステム（１１，１２）内に記憶されているデータの遠隔処理及び/又はマイクロコンピュータシステム（１１，１２）の処理モードの遠隔操作を行う、請求項１６～１９いずれか１項記載のマイクロコンピュータシステム。

21. 所定の自動的なメッセージ、例えば受信確認、伝送プロトコル、電子メールへの応答メッセージをデータ回線網（２０）を介して送信する手段が設けられている、請求項１６～２０いずれか１項記載のマイクロコンピュータシステム。

22. 種々の伝送プロトコルとデータフォーマット、例えばファックスデータ、音声データ及び/又は画像データに対する変換手段が設けられている、請求項１６～２１いずれか１項記載のマイクロコンピュータシステム。

23. 第２の端末機器（２）に対して第１の端末機器（１）から発信されたデータにアドレスデータとして名前と電話番号を添付する手段が設けられている、請求項１６～２１いずれか１項記載のマイクロコンピュータシステム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intr Application No
PCT/DE 96/02489

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/58 H04M11/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 93 20647 A (MOSS CHRISTOPHER DONALD SIBTHO) 14 October 1993 see the whole document	1-4, 14-22, 29,30
Y		5-8,11, 13,23, 24,26,28
A		9,10,12, 25,27

X	ELECTRONICS & WIRELESS WORLD, vol. 91, no. 1594, August 1985, SURREY GB, pages 33-38, XP002033518 M. ALLARD ET AL.: "Electronic Mailbox" see the whole document	1-4, 16-20
A		5-15, 21-30

	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 1997	07.07.97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Mikkelsen, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte Application No
PCT/DE 96/02489

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 379 340 A (OVEREND SEAN K ET AL) 3 January 1995 see abstract see column 3, line 7 - line 39 see column 6, line 38 - line 42	5,13,23, 28
A	---	1-3,16
Y	EP 0 413 537 A (DIGITAL EQUIPMENT INT) 20 February 1991 see abstract see column 1, line 45 - column 2, line 3	6,7

Y	WO 90 14726 A (HATTON LESLIE) 29 November 1990 see abstract see page 2, line 15 - page 3, line 26	8,24
A	---	9,10
Y	PATENT ABSTRACTS OF JAPAN vol. 016, no. 254 (E-1213), 9 June 1992 & JP 04 054756 A (NIPPON TELEGR & TELEPH CORP), 21 February 1992, see abstract	11,26

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter Application No
PCT/DE 96/02489

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9320647 A	14-10-93	NONE	
US 5379340 A	03-01-95	NONE	
EP 0413537 A	20-02-91	DE 69020457 D	03-08-95
		DE 69020457 T	14-03-96
		US 5377354 A	27-12-94
WO 9014726 A	29-11-90	DE 69006500 D	17-03-94
		DE 69006500 T	15-09-94
		EP 0473638 A	11-03-92
		JP 4507482 T	24-12-92

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国　　EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN